UNIFIED ACCESS CONTROL

IC Series Unified Access Control Appliances, UAC Agent, Junos Pulse and Enforcement Points

Product Overview

Network access control ensures users and devices are authorized to access the network and its resources, and meet security posture. Organizations need a flexible solution that protects their network investments today and in the future, supports phased deployments and grows to cover an entire enterprise. Juniper Networks is the only vendor who can deliver comprehensive, standards-based enterprise-wide access control. Juniper Networks Unified Access Control is a uniquely extensible, open solution that delivers granular access control to the entire distributed enterprise, from remote users and branch offices to the data center, while reducing cost and complexity. UAC addresses myriad network challenges such as insider threats, guest access, secure outsourcing, and regulatory compliance, while delivering scalable, adaptive access control—protecting networks, their mission-critical applications, and sensitive data.

Product Description

Juniper Networks® Unified Access Control (UAC) delivers comprehensive, granular network and application access control for even the most diverse, complex environments, reducing cost and maximizing efficiencies. UAC offers best-in-class performance and scalability with centralized policy management, simplifying deployment, administration, and management. UAC combines user identity, device security state, and network location information to create a unique, dynamic access control policy—per user and per session. UAC incorporates different levels of session-specific policy to create extremely granular access control that is easy to deploy, maintain, and dynamically modify.

Juniper Networks UAC can be enabled at Layer 2 using 802.1X, at Layer 3 using an overlay deployment, or in mixed mode using 802.1X for network admission control and a Layer 3 overlay deployment for resource access control. UAC fully integrates with any vendor's 802.1X-enabled access points or switches, including Juniper Networks EX Series Ethernet Switches which, when combined with UAC, deliver additional, rich policy enforcement capabilities. You can leverage your existing 802.1X infrastructure; any Juniper Networks firewall platform, including the SRX Series Services Gateways; or both for policy enforcement and granular access control without the need to redeploy anything. UAC also supports the Juniper Networks J Series Services Routers as Layer 3 enforcement points.

UAC is the first access control solution to support Layer 2 – Layer 7 policy enforcement with unparalleled visibility into application traffic at Layer 7 by leveraging the standalone Juniper Networks IDP Series Intrusion Detection and Prevention Appliances as UAC enforcement points.

UAC offers and operates with the UAC Agent and its agent-less mode, as well as offering and incorporating Juniper Networks Junos® Pulse, Juniper's integrated, multi-service network client which enables anytime, anywhere connectivity, security and acceleration with a simplified user experience. Standards-based Junos Pulse serves as the end user client for the multi-service, interoperable Junos Pulse Gateways, including the IC Series Unified Access Control Appliances, delivering dynamic, granular identity- and role-based network and application access control. Easy to deploy and manage, Junos Pulse enables safe, protected cloud and network access for a diverse user audience using a variety of devices.

Juniper Networks UAC is deployed quickly and easily. UAC includes an optional "step-by-step" configuration wizard to aid administrators in configuring common UAC deployment scenarios. UAC also allows you and your users to ease into policy enforcement by enabling you to phase your access control deployment and allowing it to be run in audit mode.

UAC offers industry-leading, dynamic, pre-authentication antispyware protection for Microsoft Windows endpoint devices attempting network access. UAC also provides device patch assessment checks, including endpoint inspection for targeted operating system or application hot fixes, and patch remediation services for devices that do not meet policy and require patch updates.

Juniper Networks is a strong supporter of open standards, including those of the Trusted Computing Group's (TCG) Trusted Network Connect (TNC) Work Group, which ensure interoperability with a host of network and security offerings. Through its support of the TNC standard Statement of Health (SOH) protocol, UAC interoperates with the Microsoft Windows SOH and embedded Microsoft Network Access Protection (NAP) Agents, enabling you to use your existing Microsoft Windows 7, Windows Vista and/or Windows XP SP3 clients with Juniper Networks UAC. UAC also supports the TNC's open standard Interface for Metadata Access Point (IF-MAP), enabling integration with third-party network and security devices—including nearly any device that supports the IF-MAP standard and which collects information about the happenings on or status of your network. UAC can leverage this data when formulating control decisions, taking any necessary and appropriate actions.

UAC leverages other network components to ensure secure network and application access control, address specific use cases, and centralize network policy management. UAC integrates with the standalone Juniper Networks IDP Series appliances and the SRX Series data center gateways to deliver broad application traffic visibility, mitigating insider threats by isolating threats to the user or device level and employing an applicable policy action against an offending user or device. UAC ties user identity and role information to network and application access, addressing regulatory compliance and audit demands.

UAC has also enhanced its guest user access control capabilities which provide role-based access control for guests, partners, and contractors. UAC's guest user access control delivers secure, authorized network resource access for guests, partners and contractors, manages their network use, and reduces threats from unauthorized users and compromised devices. UAC also enables enterprise selected and approved Guest User Account Managers to provision time limited temporary guest access accounts for corporate guest users.

The implementation and enforcement of consistent remote and local access control policy across a distributed enterprise is assured when UAC is deployed with Juniper Networks Network and Security Manager (NSM) and the market-leading Juniper Networks SA Series SSL VPN Appliances. UAC enables the federation of user session data between the SA Series and UAC, seamlessly provisioning SSL VPN user sessions into UAC upon login, or alternatively UAC user sessions into SSL VPN. The federation of session data between IC Series Unified Access Control Appliances and SA Series appliances is a vital part of the Location Awareness and Session Migration capabilities found within Junos Pulse. Similarly, federation allows users authenticated to one IC Series UAC Appliance to also access resources protected by another IC Series appliance on the network without reauthentication, enabling "follow-me" policies.

Juniper Networks UAC is composed of three components:

IC Series UAC Appliance

At the heart of UAC are the IC Series UAC Appliances—hardened, purpose-built, centralized policy management servers that work with Junos Pulse, the UAC Agent, or UAC's agent-less mode to obtain user authentication, endpoint security state, and device location data from a user's endpoint device. The IC Series appliances use this data to create dynamic policies that are propagated to policy enforcement points across the distributed network. The IC Series appliances manage and administer access control prior to session login and throughout the session. No forklift upgrade of existing infrastructure is required to deploy UAC.

UAC leverages Juniper's market-leading SA Series SSL VPN Appliances' policy control engine and their ability to seamlessly integrate with existing AAA/identity and access management infrastructure. IC Series appliances also feature integrated RADIUS capabilities and enhanced services from Juniper Networks SBR Enterprise Series Steel-Belted Radius Servers, which support an 802.1X transaction when an endpoint attempts network connection. The IC Series UAC Appliances may also be licensed as standalone RADIUS servers, too.

You can implement access control quickly and simply within your heterogeneous network by deploying a single IC Series UAC Appliance with your existing vendor-agnostic 802.1X switches or access points, Juniper Networks EX Series switches, Juniper Networks firewalls including the SRX Series Services Gateways, or J Series routers.

IC Series appliances are available in several different form factors. Juniper Networks IC4500 Unified Access Control Appliance addresses the access control needs of medium to large organizations or remote and branch offices. It scales to handle thousands of simultaneous endpoints and may be deployed in cluster pairs for high availability (HA). Juniper Networks IC6500 Unified Access Control Appliance is designed for use in large organizations and government agencies, offering the capacity to handle tens of thousands of simultaneous endpoints. The IC6500 FIPS meets the needs of the most demanding and complex government agencies and secure enterprise environments—offering the same functionality available on the IC6500 appliance, while adding a dedicated FIPS 140-2 Level 3 certified hardware security module to handle all cryptographic operations. These devices offer a number of redundant and HA features, including dual, hot swappable mirrored SATA hard drives, dual, hot swappable fans, and, as an option, dual, hot swappable power supplies (IC6500 and IC6500 FIPS). The IC6500 and IC6500 FIPS may be deployed in multi-unit clusters to increase performance and provide additional scalability, able to handle

multiple tens of thousands of simultaneous endpoints. Also, with UAC's adoption of the TNC's IF-MAP open, standard specification, the IC4500, IC6500, and IC6500 FIPS can serve as mixed UAC policy managers and Metadata Access Point (MAP) servers (with at least 50 concurrent user license minimum), or as standalone MAP servers (through a separate, dedicated IF-MAP license), extending UAC's integration with third-party network and security devices.

Also, the IC4500, IC6500 and IC6500 FIPS (with UAC 3.0 R2) have met the target assurance level of EAL3+ (augmented with ALC_FLR.2), and this evaluation was conducted in accordance with the Common Criteria.

UAC Agent and Junos Pulse

The UAC Agent is a dynamically downloadable agent that can be preconfigured through the Odyssey Client Administrator, provisioned in real time by the IC Series, installed using Juniper's Installer Service, delivered via Systems Management Server (SMS), or deployed by other distribution means. The same UAC Agent can be used in wired, wireless, or combined deployments. The UAC Agent is also available as a cross-platform, dynamically downloadable lightweight agent. UAC also supplies an agent-less mode for circumstances where the download of software is not feasible. The UAC Agent can be delivered based on role, linking agent-based or agent-less access dynamically to user or device identity. The UAC Agent collects user and device credentials, and assesses the endpoint's security state. It delivers integrated 802.1X functionality from Juniper Networks Odyssey Access Client (OAC)—an 802.1X client/supplicant—as well as Layer 3-7 functionality, including an integrated personal firewall for dynamic client-side policy enforcement. It also includes specific functionality for Microsoft Windows devices such as IPsec VPN as an optional secure transport using IPsec to enable encryption from the endpoint to a firewall for session integrity and privacy, and single sign-on (SSO) to Microsoft Active Directory. The UAC Agent's integrated Host Checker functionality, which is used in thousands of SA Series SSL VPN deployments, enables you to define policy that scans endpoints attempting to connect to your network for a variety of security applications and states—including antivirus, antimalware, and personal firewalls. It also enables custom checks of elements such as registry and port status, and can perform an MD5 checksum to verify application validity. UAC also offers industry-tested, dynamic antispyware/antimalware protection for Microsoft Windows endpoint devices that attempt network access, scanning device memory, registry and load points, pre-authentication, for spyware and keyloggers. The UAC Agent's Host Checker can also assess an endpoint during machine authentication, mapping the device to a different role and placing it into remediation based on assessment results. Deployment is simplified through predefined Host Checker policies and the automatic monitoring of antivirus and antispyware signatures and patches for the latest definition files for posture assessment. Supporting the most popular enterprise computing platforms, the UAC Agent delivers cross-platform support, including Layer 2 and Layer 3 authentication and endpoint integrity for devices running Microsoft Windows 7 Enterprise, Windows Vista (32- and 64-bit), Windows XP, and Windows 2000 operating systems, as well as devices running Apple Mac OS operating system software.

Juniper also offers Junos Pulse as an option for UAC customers with Microsoft Windows based devices. Like the UAC Agent, Junos Pulse deployed with UAC delivers granular access control based on user identity and role, device type and integrity, and location. UAC customers are able select a dynamic download of Junos Pulse or the UAC Agent from their IC Series appliance. Junos Pulse operates like the UAC Agent, gathering user and device credentials, and checking an endpoint's security status. Junos

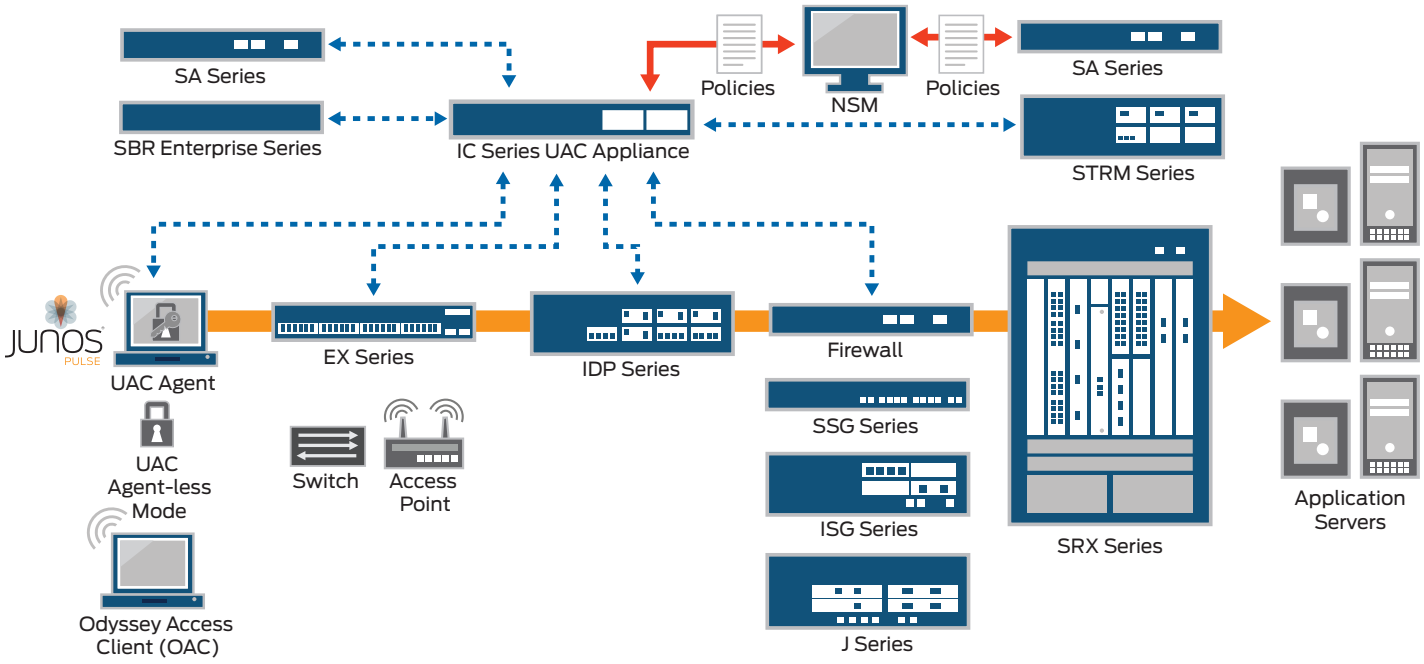

Figure 1: Standards-based Juniper Networks Unified Access Control (UAC) works with existing and new network components to deliver comprehensive network and application access control

Pulse also includes Host Checker functionality as well as offering dynamic antispyware/antimalware protection for Microsoft Windows based devices, like the UAC Agent. Junos Pulse, though, leverages and integrates with the native 802.1X supplicant available within the Microsoft Windows operating systems to deliver Layer 2 access control, in addition to delivering Layer 3 authentication and IPsec tunneling with any Juniper Networks firewall including the SRX Series gateways.

UAC Enforcement Points

UAC enforcement points include any 802.1X compatible wireless access point and switch, including the Juniper Networks EX2200, EX3200, EX4200 and EX8200 line of switches; any Juniper Networks firewall/VPN platform; J Series Services Routers (running up to Junos OS 10.4); and standalone IDP Series appliances, as well as SRX Series gateways providing role-based, application-level policy enforcement. Juniper Networks firewall products, including the SRX Series, Juniper Networks SSG Series Secure Services Gateways, and Juniper Networks ISG Series Integrated Security Gateways act as Layer 3-7 overlay enforcement points for UAC. For organizations desiring Layer 2 port-based enforcement, UAC's support for vendor-agnostic 802.1X switches and wireless access points enables them to quickly realize the benefits of access control without requiring a hardware overhaul. The EX Series switches, when used in conjunction with UAC, can apply quality of service (QoS) policies or mirror user traffic to a central location for logging, monitoring, or threat detection with intrusion prevention systems. J Series routers may also serve as Layer 2 UAC enforcement points. And, with Juniper's standalone IDP Series appliances serving as role-based application-level policy enforcement points, UAC is able to deliver access control to the application layer within your network.

Many Juniper Networks firewalls also support unified threat management (UTM) capabilities including IPS functionality, network-based antivirus, antispam, anti-adware, antiphishing, and URL filtering capabilities. This functionality can be dynamically leveraged as part of UAC to enforce and unify access control and security policies on a per user and per session basis, delivering comprehensive network access and threat control. UAC enforcement points may also be implemented in transparent mode, which requires no rework of routing and policies, or changes to the network infrastructure. They may also be set up in audit mode to determine policy compliance without enforcement, enabling you and your users to ease into access control.

Features and Benefits

Table 1: Advanced Network and Application Protection

Juniper Networks UAC is a self-administering platform which intelligently quarantines non-compliant users and devices, and delivers extended remediation capabilities. It enables the automatic quarantine and remediation of users and devices that do not meet access and security policies prior to granting network access, as well as users and devices that do not adhere to policy during their network session. UAC also delivers automatic remediation for non-compliant devices, many times without user intervention or other assistance. UAC's self-administering platform saves time and cost, while increasing user and support staff productivity by minimizing user downtime and help desk calls.

Features	Feature Description	Benefits
Role-based application-level enforcement	• Leverages standalone IDP Series appliances as enforcement points • Enables application-specific policy rules to be enforced via any level of policy granularity • Policies can also be defined to control time of day and bandwidth restrictions per application or per role	• The first access control solution to support full Layer 2 - Layer 7 enforcement • Enables access control and security policies to be applied to the application-level, granularly protecting your network, applications, and data • Ensures that users adhere to application usage policies, controlling access to applications such as instant messaging, peer-to-peer, and other corporate applications
Automated patch assessment checks and remediation	• Provides device patch assessment checks through OEM integration of Shavlik Technologies' Shavlik NetChk Protect predefined patch assessment technologies, including endpoint inspection for targeted operating systems or application hot fixes • Can tie access directly to the presence or absence of specific hot fixes for defined operating systems and applications, and performs role-based, predefined patch management checks according to vulnerability severity level • Installed Systems Management Server (SMS) or System Center Configuration Manager (SCCM) 2007 can be leveraged to automatically check for patch updates, quarantining, remediating, and providing authorized network access once a device has been remediated • Shavlik's automatic patch remediation capabilities are available, which enables specific patches to be identified and applied, if needed. Shavlik NetChk Protect provides Microsoft patches and supports patches for non-Microsoft products, directly downloading missing patches from the appropriate vendor's website. Internet connectivity is required for Shavlik remediation to work	• Enables more enhanced, granular endpoint device health and security state assessments • Minimizes user interaction and downtime through automatic remediation and management of patches for endpoint devices, reducing help desk calls

Table 1: Advanced Network and Application Protection (continued)

Features	Feature Description	Benefits
Dynamic antispyware/ antimalware protection	• Offers industry-leading, dynamic antispyware/antimalware protection from market-leader Webroot which, before authentication, scans the memory, registry and load points of an endpoint device for spyware, keyloggers and other malware • Ties into UAC's existing granular policy management framework to allow administrators to quarantine or restrict network access of infected devices • Spyware signatures are automatically downloaded and updated • Works with all Windows-based UAC Agents and Junos Pulse, as well as in UAC's agent-less mode • Antispyware/antimalware is also available in SA Series SSL VPN Appliances	• Ensures unmanaged and managed Windows devices are not running spyware, keyloggers or other malware before authentication • Quarantines or restricts device access through UAC's existing granular policy management framework
Coordinated Threat Control	• Leverages robust features and capabilities of the standalone IDP Series appliances and Juniper Networks SRX3400, SRX3600, SRX5600 and SRX5800 Services Gateways to deliver broad Layer 2 - Layer 7 visibility into application traffic • Isolates a threat down to the user or device level—in conjunction with the IDP Series appliances and SRX3400, SRX3600, SRX5600 and SRX5800 gateways—and employs a specific, configurable policy action against the offending user or device	• Addresses and mitigates network insider threats quickly and simply • Minimizes network and user downtime
Captive Portal	• If a user attempts unauthorized network access via a web browser, administrators have an option to redirect the user to an IC Series appliance for authentication • Once the user logs in to the IC Series appliance with appropriate credentials, the IC Series will redirect the web browser back to the original resource from which it had been redirected	• Redirects users to login to the IC Series appliance before they can reach their desired resource within the network, providing further network protection

Table 2: Identity-Enabled Network and Application Control, Visibility, and Monitoring

UAC correlates user identity and role information to network and application security and usage. With UAC, you will know who is accessing your network and applications, when your network and applications are being accessed, what is being accessed, and where the user and device has been on your network. UAC provides valuable, effective tracking and auditing of network and application access, which helps address regulatory compliance requirements and audits.

Features	Feature Description	Benefits
Federation – UAC – SA Series and IC Series – IC Series	• Federation of user sessions between SA Series SSL VPN Appliances and UAC enables seamless provisioning of SSL VPN user sessions into UAC upon login, or alternatively UAC user sessions into SSL VPN at login • Users authenticated to one IC Series appliance may, if authorized, access resources protected by another IC Series UAC Appliance, enabling "follow-me" policies • UAC leverages the Trusted Computing Group's (TCG) Trusted Network Connect (TNC) standard protocol Interface for Metadata Access Point (IF-MAP) to enable federation	• Provides users—whether remote or local— with seamless access to corporate resources protected by uniform access control policies through a single login, offering a consistent user access experience • Enables the Location Awareness and Session Migration capabilities of Junos Pulse
Role-based Unified Threat Management (UTM) policy application	Create and apply role-based threat management policies, such as network IPS, network antivirus, network antispyware, and/or network URL filtering	Delivers dynamic access control *and* dynamic threat control
Identity-enabled data center and branch firewalling	• Combines UAC's identity-aware capabilities with the robust networking and security services of the SRX Series Services Gateways • Enables SRX Series gateways to be employed as UAC enforcement points • Adds "Username" and "Role" information to the SRX Series Services Gateways' logs, enhancing monitoring, troubleshooting, and regulatory compliance • Available on all SRX Series Services Gateways running Juniper Networks Junos® operating system 9.4 or higher	• Drastically increases scalability for data center environments and branch office alike • Enables organizations to leverage enforcement in the world's most demanding and high-performance data centers

Table 3: Standards-Based, Interoperable Access Control

Juniper Networks UAC provides standards-based, vendor-agnostic access control and seamless support for existing, heterogeneous network environments. UAC leverages industry-standards including 802.1X, RADIUS, and IPsec, as well as innovative, open standards, such as the Trusted Network Connect's (TNC) standards for network access control and network security, delivering a comprehensive, standards-based access control solution. UAC has been built on industry leading products, including the policy engine, AAA capabilities, and host checking of Juniper Networks SA Series SSL VPN Appliances, RADIUS capabilities from SBR Enterprise Series Steel-Belted Radius Servers, 802.1X capabilities from OAC in the UAC Agent, and interoperability with the Microsoft Windows native 802.1X client/supplicant for Junos Pulse. Standards-based UAC facilitates quick, simple, and flexible access control deployments, delivers investment protection, time and cost savings, and alleviates single vendor lock-in.

Features	Feature Description	Benefits
Junos Pulse	• Integrated, multi-service network client that enables anytime, anywhere connectivity, security and acceleration with a simplified user experience • When deployed as the client for UAC, delivers dynamic, granular identity- and role-based network access control (NAC) • Leverages existing 802.1X client/supplicant native to Microsoft Windows to deliver Layer 2 access control • Delivers Layer 3 authentication and IPsec tunneling with Juniper firewalls and SRX Series Services Gateways • Supports Microsoft Windows XP, Vista (32- and 64-bit) and Windows 7 (32- and 64-bit)	• Delivers granular access control based on user identity and role, device type and integrity, and location • Helps identify who is accessing a network and its applications, when, how, from where, and by what device
TNC open standards support	Adopts and provides strong support for the TCG's TNC open standards for network access control and security	• Enables choice by empowering organizations to select endpoint and network security solutions that meet their needs without concern for interoperability • Enables ease-of-deployment, leading to faster ROI
IF-MAP support	• Adopts and utilizes the TNC's open standard IF-MAP • Enables integration with third-party network and security devices, including devices that collect and through IF-MAP, share information on the state and status of a network, user or device • Allows devices to report back to the IC Series appliances serving as MAP (Metadata Access Point) servers, enabling the collected data to be used in formulating policies and appropriate access actions • Enables IC Series appliances to serve as standalone MAP servers (through a separate, dedicated IF-MAP license), or as mixed IC Series appliances and MAP servers (with at least a 50 concurrent user license) • Supports a MAP server running on standalone IC Series or in active/passive cluster pairs	• Integrates existing, third-party network and security devices into the access control platform • Enhances visibility into the state of and actions on or by a network, user and device—and collects and incorporates that data into the access control policy decision process
Windows Statement of Health (SOH) and embedded NAP agent support	• Allows organizations—through the TNC SOH standard—to leverage their pre-installed Microsoft Windows 7, Windows Vista and XP SP3 clients with UAC for access control • Allows the use of the Windows Security Center (WSC) SOH in access control decisions • Can pass the SOH to a Microsoft NPS server for external enforcement and validation of the SOH and transmit the information back to the IC Series for use in access control decisions	• Streamlines client deployment • Simplifies access control rollout and implementation
EX Series Ethernet Switch interoperability	• EX2200, EX3200, EX4200 and EX8200 interoperate with and serve as enforcement points within UAC—using standards-based 802.1X port-level access control and Layer 2-4 policy enforcement • When deployed with UAC, EX Series switches can enforce user-based QoS policies, or mirror user traffic to a central location for logging, monitoring, or threat detection	Delivers a complete, standards-based, best-in-class network access control (NAC) solution, allowing organizations to enjoy value-added features and economies of scale for support and service
FIPS Compliance	• IC6500 FIPS offers the same functionality as the IC6500 UAC Appliance while adding a dedicated FIPS 140-2 Level 3 certified hardware security module (HSM) to handle all cryptographic operations, and tamper evident labels to deter physical security breaches and provide a visual indication of device integrity • Can be deployed with OAC FIPS Edition (using Juniper Networks Odyssey Security Component cryptographic module FIPS 140-2 Level 1, Certificate #569, conforming to NIST and DoD guidelines for the use of 802.11i and TLS-based EAP methods)	Enables agencies to deploy comprehensive, scalable network access control which meets government approved standards
Common Criteria Acceptance	IC Series UAC Appliances (with UAC 3.0 R2) meet the target assurance level of EAL3+ (augmented with ALC_FLR.2), with this evaluation conducted in accordance with the Common Criteria.	Adheres to U.S. government and international regulatory standards in delivering robust, standards-based network access control (NAC)

Table 4: Simple, Flexible Deployment

The innovative design of the standards-based Juniper Networks UAC enables organizations to begin controlling network and application access quickly and simply. Organizations are encouraged to initiate network access control with UAC in a phased approach, beginning with a small deployment and growing to support hundreds of thousands of concurrent users through UAC's unparalleled scalability. Organizations may also wish to initially deploy UAC in audit mode, which enables an organization to track user and device policy compliance without enforcing policies. This allows users and administrators alike to become familiar with access control policies and enables the organization to phase in policy compliance enforcement. This approach ultimately saves access control deployment time and cost.

Features	Feature Description	Benefits
Guest Access support	• One-time guest user accounts available • Guest user accounts may also be provisioned with a predefined timeout period • Administrators control the maximum time duration allowed • Allows reception and other non-technical enterprise employees to host/provision secure guest user accounts dynamically through easy-to-use guest user account management	Enhances and simplifies an organization's ability to provide secure, differentiated guest user access to their networks
Centralized policy management	• Centralized policy management is delivered when UAC is deployed with Network and Security Manager (NSM) and SA Series • Common configuration templates can be shared between SA Series (remote access control) and UAC (network access control) deployments using NSM • NSM also provides a single management server that can configure key components of a UAC deployment	• Saves administrative time and cost, and offers a consistent user and administrative experience by delivering common remote and local access control policy implementation and enforcement across a distributed enterprise • Makes possible and simplifies enterprise-wide deployment of uniform access control policies
Common Access Licensing	• Requires only user licenses (with appropriate IC Series appliance) to initiate access control • User licenses can either be used for concurrent user sessions on the IC Series UAC Appliances, or the SA Series SSL VPN Appliances	• Simplifies the product licensing model that can be used across UAC and the SA Series appliances • Please see the Ordering Information section for the new common access license SKUs that can now be used for the IC Series and SA Series appliances
Wizard-based Configuration	• An optional, step by step configuration wizard to aid administrators in the configuration of five of the most common UAC deployment scenarios, including: - System Setup - RADIUS Configuration - Guest User Management - UAC Layer 2 Enforcement - UAC Layer 3 Enforcement • Tasks for a given deployment scenario are arranged in a well-defined, dependent order • Wizard-based configuration admin UI navigates to the corresponding configuration screen when the administrator clicks on a particular task	Aids administrators in navigating and familiarizing themselves with configuration tasks in the UAC Admin UI
Dynamic authentication policy	• Leverages an organization's existing investments in directories, PKI, and strong authentication • Supports 802.1X, RADIUS, LDAP, Microsoft Active Directory, RSA Authentication Manager, Network Information Service (NIS), certificate servers (digital certificates/PKI), local login/password, CA SiteMinder, RSA ClearTrust, Oblix (Oracle), and RADIUS Proxy	• Saves time and expense by leveraging and interfacing with existing AAA infrastructures • Establishes a dynamic authentication policy for each user session • Enables support—through RADIUS Proxy—for deployments where certain authentications are supported by a backend RADIUS server
Dynamically addresses unmanageable endpoint devices	Employs media access control (MAC) address authentication via RADIUS, in combination with MAC address whitelisting and blacklisting; or, leverages existing policy and profile stores (through LDAP interfaces) or asset discovery or profiling solutions for role- and resource-based access control of unmanageable devices—such as networked printers, cash registers, bar code scanners, VoIP handsets, etc.	• Enhances network and application protection • Makes it simpler and faster for organizations to deploy access control across their entire network regardless of device manageability • Saves time and cost

Table 4: Simple, Flexible Deployment (continued)

Features	Feature Description	Benefits
UAC Agent and Junos Pulse localization	• Provides localized UI, online help, installer, and documentation for the UAC Agent and Junos Pulse, supporting the following languages: - Chinese (Simplified) - Chinese (Traditional) - French - German - Japanese - Korean - Spanish	Enables organizations with users not proficient in English to effectively deploy and employ UAC across their distributed enterprise
Granular auditing and logging	• Provides fine-grained auditing and logging capabilities, including access to the IC Series RADIUS diagnostic log files, delivered in a clear, easy-to-understand format • Captures detailed logging by roles that users belong to, resources that they are trying to access, and the state of compliance of the endpoint and user to the security policies of the network	• Simplifies the diagnosis and repair of network issues that arise • Addresses industry and government regulatory compliance and audits
RADIUS Only Appliance	• Utilizes many of the features and functions found within the SBR Series servers as a basis for its AAA and RADIUS capabilities. • New license enables organizations desiring only a RADIUS appliance to access only the AAA/RADIUS features found on the IC Series appliances	• Enables the IC Series UAC Appliance to be deployed as a AAA/RADIUS server • Enables an organization to become familiar with the IC Series appliances • Allows an organization to upgrade to a full featured UAC license at a future date

Product Options

The IC4500, IC6500, and IC6500 FIPS have several hardware and software options available:

Table 5: Product Options

Options	Option Description	Applicable Products
Cluster Licensing Options	Customers now have the ability to build clusters without buying additional licenses. This new clustering method can be explained in two simple steps. 1. Simply place an equal number of user ("-ADD") licenses on each box. 2. When they are joined together to form a cluster, all of the user licenses add up so that the cluster can now support all of the licensed users. For example, building a 1,000 user cluster would be done by bringing two IC Series appliances together with 500 user licenses each on the two appliances. Clustering allows you to share licenses from one IC Series UAC Appliance with one or more additional IC Series appliances, depending on the platform. The licenses are not additive to the concurrent user licenses. For example, if a customer has a 1,000 user license for the IC4500 and then purchases another IC4500, this will provide a total of 1,000 users that are shared across both appliances, not per appliance. A number of High Availability clustering options have been created to support the IC Series, ensuring redundancy and seamless failover in the rare case of a system failure. Clustering also provides performance scalability to handle the most demanding usage scenarios. The IC6500 and IC6500 FIPS may be purchased in multi-unit clusters or cluster pairs to provide redundancy and expansive user scalability.	IC4500, IC6500, IC6500 FIPS
Microsoft SOH Licenses	The licensing of the System Health Agent (SHA)/System Health Verifiers (SHV) and SOH protocols from Microsoft are addressed, which are key components that enable UAC to support the Microsoft Windows SOH and embedded NAP Agent through the TNC SOH open and standardized protocol, IF-TNCCS-SOH.	IC4500, IC6500, IC6500 FIPS
UAC Disaster Recovery Licenses	UAC's Disaster Recovery licenses address disaster situations without requiring a permanent purchase of user licenses by a customer for those types of contingencies. Also, periodic testing of disaster recovery deployment is enabled while still providing usage when needed. Disaster Recovery licenses are also available for clusters.	IC4500, IC6500, IC6500 FIPS
UAC MAP Server Licenses	Leveraging the TNC's IF-MAP specification, IC Series (or IC Series appliance cluster) may operate solely as a MAP server with no additional simultaneous endpoint licenses or OAC-ADD-UAC licenses. In this mode, the IC Series (or clustered IC Series appliances) as MAP servers must have a MAP Server license installed. Mixed IC Series and MAP server mode is defined as any IC Series appliance that simultaneously acts as both an IC Series appliance and as a MAP server, where either a simultaneous endpoint license or an OAC-ADD-UAC license has been installed. In this case, the MAP Server license is not required on that IC Series appliance (or IC Series appliance cluster).	IC4500, IC6500, IC6500 FIPS
Enhanced Endpoint Security (EES) Subscription Licenses	In UAC, the Enhanced Endpoint Security system now offers antispyware/antimalware functionality to ensure that unmanaged and managed Microsoft Windows endpoint devices are not running spyware or keyloggers. Spyware contaminated devices may be quarantined or have restricted end user access based on policy enforcement. Scans an endpoint's memory, registry and load points for spyware and malware. A base UAC license includes a free Enhanced Endpoint Security user license for two (2) simultaneous users, allowing users to "try before they buy." Subscription licenses for additional Enhanced Endpoint Security users are available.	IC4500, IC6500, IC6500 FIPS
RADIUS Only Licenses	License enables organizations that wish to deploy a RADIUS appliance access to only the AAA/RADIUS features of the IC Series appliance, while introducing the organization to the IC Series appliances, as well as allowing the organization to upgrade to a full featured UAC license at a future date.	IC4500, IC6500, IC6500 FIPS
Hot swappable hard disk drives	Dual, mirrored hot swappable SATA hard drives.	IC6500, IC6500 FIPS
Hot swappable power supplies	Optional dual, hot swappable power supplies. IC6500 FIPS – Second power supply optional, DC power supplies available.	IC6500, IC6500 FIPS
Dual, hot swappable fans	Dual, hot swappable fans.	IC6500, IC6500 FIPS
Four-port 10/100/1000 copper interface card (Standard)	Four-port 10/100/1000 copper interface card (standard).	IC6500 FIPS

IC4500

IC6500 / IC6500 FIPS

Specifications

	IC4500	IC6500 / IC6500 FIPS
Dimensions and Power		
Dimensions (W x H x D)	17.26 x 1.75 x 14.5 in (43.8 x 4.4 x 36.8 cm)	17.26 x 3.5 x 17.72 in (43.8 x 8.8 x 45 cm)
Weight	15.6 lb (7.1 kg) typical (unboxed)	26.4 lb (12 kg) typical (unboxed) (IC6500) 26.9 lb (12.2 kg) typical (unboxed) (IC6500 FIPS)
Rack mountable	Yes, 1U	Yes, 2U, 19 in
A/C power supply	100-240 VAC, 60-50 Hz, 2.5 A Max, 300 W	100-240 VAC, 60-50 Hz, 2.5 A Max, 400 W
System battery	CR2032 3V lithium coin cell	CR2032 3V lithium coin cell
Efficiency	80% minimum, at full load	80% minimum, at full load
Material	18 gauge (.048") cold-rolled steel	18 gauge (.048 in) cold-rolled steel
Fans	Three 40 mm ball-bearing fans, One 40 mm ball-bearing fan in power supply	Two 80 mm hot swap, One 40 mm ball-bearing fan in power supply
Panel Display		
Power LED, HD activity, HW alert	Yes	Yes
PS fail	No	Yes
HDD activity and RAID status LEDs	No	Yes
Ports		
Traffic	Two RJ-45 Ethernet - 10/100/1000 full or half duplex (auto-negotiation)	Four RJ-45 Ethernet – full or half-duplex (auto-negotiation) (IC6500) Four-port 10/100/1000 copper interface card (IC6500 FIPS)
Fast Ethernet	IEEE 802.3u compliant	IEEE 802.3u compliant
Gigabit Ethernet	IEEE 802.3z or IEEE 802.3ab compliant	IEEE 802.3z or IEEE 802.3ab compliant
Console	One RJ-45 serial console port	One RJ-45 serial console port
Environment		
Operating temp	41º to 104º F (5º to 40º C)	41º to 104º F (5º to 40º C)
Storage temp	-40º to 158º F (-40º to 70º C)	-40º to 158º F (-40º to 70º C)
Relative humidity (operating)	8% to 90% noncondensing	8% to 90% noncondensing
Relative humidity (storage)	5% to 95% noncondensing	5% to 95% noncondensing
Altitude (operating)	10,000 ft (3,048 m) maximum	10,000 ft (3,048 m) maximum
Altitude (storage)	40,000 ft (12,192 m) maximum	40,000 ft (12,192 m) maximum
Certifications		
Safety certifications	EN60950-1:2001+ A11, UL60950-1:2003, CAN/CSA C22.2 No. 60950-1-03, IEC 60950-1:2001	EN60950-1:2001+ A11, UL60950-1:2003, CAN/CSA C22.2 No. 60950-1-03, IEC 60950-1:2001
Emissions certifications	FCC Class A, EN 55022 Class A, EN 55024 Immunity, EN 61000-3-2, VCCI Class A	FCC Class A, EN 55022 Class A, EN 55024 Immunity, EN 61000-3-2, VCCI Class A
Warranty	90 days; Can be extended with support contract	90 days; Can be extended with support contract

UAC Agent, Junos Pulse and UAC Agent-less Mode – Specifications

- The Layer 2 UAC Agent (802.lX supplicant) supports Microsoft Windows 7 (32- and 64-bit), Windows Vista SP2 (32- and 64-bit), and Windows XP SP3 operating systems, and Apple Mac OS operating system software.
- The Layer 3 UAC Agent (full client) supports Microsoft Windows 7 (32- and 64-bit), Windows Vista SP2 (32- and 64-bit), and Windows XP SP3 operating systems , and Apple Mac OS operating system software. The Layer 3 UAC Agent (Java based) supports Microsoft Windows XP SP3, Apple Mac OS operating system software, and Linux operating platforms, including Fedora, Ubuntu, and openSUSE.
- The UAC agent-less mode secures devices running Microsoft Windows 7 (32- and 64-bit), Windows Vista SP2 (32- and 64-bit), and Windows XP SP3 operating systems, Apple Mac OS and Linux operating systems and platforms including Fedora, Ubuntu and openSUSE, interoperating with supported browsers including Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari.
- Junos Pulse deployed with/by UAC supports Microsoft Windows 7 (32- and 64-bit), Windows Vista SP2 (32- and 64-bit), and Windows XP SP3 operating systems.

For specific, supported operating system software, operating platform, and browser versions please refer to the latest version of the Unified Access Control Supported Platforms document, which may be found at **www.juniper.net/techpubs/software/uac/**.

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services**.

Ordering Information

Model Number	Description
IC4500	
Base System	
IC4500	IC4500 base system
Endpoint Licenses (Common Access Licenses)	
ACCESSX500-ADD-25U	Add 25 simultaneous endpoints to ICx500 or SAx500
ACCESSX500-ADD-50U	Add 50 simultaneous endpoints to ICx500 or SAx500
ACCESSX500-ADD-100U	Add 100 simultaneous endpoints to ICx500 or SAx500
ACCESSX500-ADD-250U	Add 250 simultaneous endpoints to ICx500 or SAx500
ACCESSX500-ADD-500U	Add 500 simultaneous endpoints to ICx500 or SAx500
ACCESSX500-ADD-1000U	Add 1,000 simultaneous endpoints to ICx500 or SAx500
ACCESSX500-ADD-2000U	Add 2,000 simultaneous endpoints to ICx500 or SAx500
ACCESSX500-ADD-3000U	Add 3,000 simultaneous endpoints to ICx500 or SAx500
ACCESSX500-ADD-5000U	Add 5,000 simultaneous endpoints to ICx500 or SAx500
Feature Licenses	
IC4500-OAC-ADD-UAC	Add UAC support to Odyssey Access Clients on IC4500
Disaster Recovery Licenses	
IC4500-DR	Disaster recovery license for IC4500
IC4500-DR-CL	Disaster recovery license for IC4500 cluster
Microsoft SOH License	
IC4500-SOH	Microsoft SOH license for IC4500
IF-MAP License	
IC4500-IFMAP	IF-MAP license for IC4500
IC4500-IFMAP-CL	IF-MAP license for IC4500 cluster
RADIUS Only License	
IC4500-RADIUS-SERVER	Add RADIUS Server Feature to the IC4500
IC6500	
Base System	
IC6500	IC6500 base system
Endpoint Licenses (Common Access Licenses)	
ACCESSX500-ADD-100U	Add 100 simultaneous endpoints to ICx500 or SAx500
ACCESSX500-ADD-250U	Add 250 simultaneous endpoints to ICx500 or SAx500
ACCESSX500-ADD-500U	Add 500 simultaneous endpoints to ICx500 or SAx500
ACCESSX500-ADD-1000U	Add 1,000 simultaneous endpoints to ICx500 or SAx500
ACCESSX500-ADD-2000U	Add 2,000 simultaneous endpoints to ICx500 or SAx500
ACCESSX500-ADD-3000U	Add 3,000 simultaneous endpoints to ICx500 or SAx500
ACCESSX500-ADD-5000U	Add 5,000 simultaneous endpoints to ICx500 or SAx500
ACCESSX500-ADD-10000U	Add 10,000 simultaneous endpoints to ICx500 or SAx500
ACCESSX500-ADD-15000U	Add 15,000 simultaneous endpoints to ICx500 or SAx500

Model Number	Description
Endpoint Licenses (Common Access Licenses) (continued)	
ACCESSX500-ADD-20000U	Add 20,000 simultaneous endpoints to ICx500 or SAx500
ACCESSX500-ADD-25000U	Add 25,000 simultaneous endpoints to ICx500 or SAx500
ACCESSX500-ADD-30000U	Add 30,000 simultaneous endpoints to ICx500 or SAx500
Feature Licenses	
IC6500-OAC-ADD-UAC	Add UAC support to Odyssey Access Clients on IC6500
Disaster Recovery Licenses	
IC6500-DR	Disaster recovery license for IC6500
IC6500-DR-CL	Disaster recovery license for IC6500 Cluster
Microsoft SOH License	
IC6500-SOH	Microsoft SOH license for IC6500
IF-MAP License	
IC6500-IFMAP	IF-MAP license for IC6500 /IC6500 FIPS
IC6500-IFMAP-CL	IF-MAP license for IC6500 /IC6500 FIPS cluster
RADIUS Only License	
IC6500-RADIUS-SERVER	Add RADIUS Server Feature to the IC6500
IC6500 FIPS	
Base System	
IC6500FIPS	IC6500 FIPS base system
Endpoint Licenses (Common Access Licenses)	
Please refer to IC6500 endpoint licenses ordering information on previous page.	
Feature Licenses	
Please refer to IC6500 feature licenses ordering information.	
Disaster Recovery Licenses	
Please refer to IC6500 disaster recovery licenses ordering information.	
Microsoft SOH License	
Please refer to IC6500 Microsoft SOH license ordering information.	
RADIUS Only License	
Please refer to IC6500 RADIUS Only License ordering information.	

Model Number	Description
Enhanced Endpoint Security (EES) Subscription Licenses	
ACCESS-EES-50U-1YR	50 Concurrent Users, 1 Year
ACCESS-EES-100U-1YR	100 Concurrent Users, 1 Year
ACCESS-EES-250U-1YR	250 Concurrent Users, 1 Year
ACCESS-EES-500U-1YR	500 Concurrent Users, 1 Year
ACCESS-EES-1000U-1YR	1,000 Concurrent Users, 1 Year
ACCESS-EES-2500U-1YR	2,500 Concurrent Users, 1 Year
ACCESS-EES-5000U-1YR	5,000 Concurrent Users, 1 Year
ACCESS-EES-7500U-1YR	7,500 Concurrent Users, 1 Year
ACCESS-EES-50U-2YR	50 Concurrent Users, 2 Years
ACCESS-EES-100U-2YR	100 Concurrent Users, 2 Years
ACCESS-EES-250U-2YR	250 Concurrent Users, 2 Years
ACCESS-EES-500U-2YR	500 Concurrent Users, 2 Years
ACCESS-EES-1000U-2YR	1,000 Concurrent Users, 2 Years
ACCESS-EES-2500U-2YR	2,500 Concurrent Users, 2 Years
ACCESS-EES-5000U-2YR	5,000 Concurrent Users, 2 Years
ACCESS-EES-7500U-2YR	7,500 Concurrent Users, 2 Years
ACCESS-EES-50U-3YR	50 Concurrent Users, 3 Years
ACCESS-EES-100U-3YR	100 Concurrent Users, 3 Years
ACCESS-EES-250U-3YR	250 Concurrent Users, 3 Years
ACCESS-EES-500U-3YR	500 Concurrent Users, 3 Years
ACCESS-EES-1000U-3YR	1,000 Concurrent Users, 3 Years
ACCESS-EES-2500U-3YR	2,500 Concurrent Users, 3 Years
ACCESS-EES-5000U-3YR	5,000 Concurrent Users, 3 Years
ACCESS-EES-7500U-3YR	7,500 Concurrent Users, 3 Years
Accessories	
IC6500-PS	Field upgradeable secondary power supply for IC6500 /IC6500 FIPS
SA-ACC-RCKMT-KIT-1U	SA Series and IC Series rack mount kit - 1U
SA-ACC-RCKMT-KIT-2U	SA Series and IC Series rack mount kit - 2U
SA-ACC-PWR-AC-UK	SA Series and IC Series AC power cord UK
SA-ACC-PWR-AC-EUR	SA Series and IC Series AC power cord EUR
SA-ACC-PWR-AC-JPN	SA Series and IC Series AC power cord JPN

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

1000137-010-EN Nov 2011 Printed on recycled paper